

### **Amendments to the Specification:**

In the office action mailed November 20, 2007 the Examiner objected to the specification because it contains an embedded hyperlink and/or other form of browser executable code.

In accordance with 37 CFR 1.57(d), please amend the specification as follows to remove all embedded hyperlinks.

On page 1 after the title “Background of the Invention”, please replace the paragraph that begins with “Commerce over computer networks has become very popular...” with the following:

Commerce over computer networks has become very popular. Such commerce takes many forms, from purchasing books and merchandize from on-line vendors such as books from amazon.com and hockey equipment from epuck.com to conducting online banking and stock trading. Common to all such transactions is the need to communicate private secure information. Typically, the transactions are carried out over secure encrypted connections. However, there are still opportunities for the devious to contrive schemes to capture the private information that is used during online transactions, for example, to obtain passwords, personal identification numbers (PIN), Social Security Numbers, driver's license numbers and account numbers. Illegal procurement of such information and using such information in a fraudulent manner is commonly referred to as *identity theft*. According to the Federal Trade Commission, in the year 2002 alone, there were 9.9 million identity theft victims. The thefts cost businesses \$47.6 billion and \$5 billion in out-of-pocket expenses to individuals in 2002 (Federal Trade Commission, “Federal Trade Commission Identity Theft Survey Report,” September 2003, <http://www.ftc.gov/os/2003/09/synovatereport.pdf>).

On page 2 beginning at line 9, please replace the paragraph that begins with “One form of conducting online identity theft is to use keystroke logger to..” with the following:

One form of conducting online identity theft is to use keystroke logger to log individual keystrokes and to extract information, such as password and credit card number, from the logs. Two known cases are the Kinko’s case in New York and the Boston College case (Jesdanun, A., “Thief captures every keystroke to access accounts,” Seattle Post, July, 2003, [http://seattlepi.nwsource.com/national/131961\\_snoop23.html](http://seattlepi.nwsource.com/national/131961_snoop23.html); Poulsen, K., “Guilty Plea in Kinko's Keystroke Caper,” SecurityFocus, July 18, 2003 <http://www.securityfocus.com/printable/news/6447>). In both cases, the thieves installed keystroke logger software in public Internet computers, in Kinko’s stores or in the college campus. They captured user ID’s, user names, and passwords, using them to access or even open bank accounts online, making purchases, and entering buildings illegally.

On page 4 beginning with line 17, please replace the paragraph that begins “Another form of protecting the security of online commerce is the authentication of an individual involved...” with the following:

Another form of protecting the security of online commerce is the authentication of an individual involved in a transaction, for example, though identity federation or federation of authentication, such as Kerberos (“Kerberos: The Network Authentication Protocol,” <http://web.mit.edu/kerberos/www/>) and Microsoft Passport (*Microsoft .Net Passport*, Microsoft Cooperation, <http://www.passport.net/>). However, these mechanisms also do not protect against keyboard loggers and similar schemes.